Abstract

In a method of returning change to a payer in an electronic payment system, a payer determines a change return value, generates and blinds a change return certificate, generates

5   a first signature by signing the blinded change return certificate, and sends a message comprising the first signature to a payee. The payee forwards the message to a payment provider. The payment provider verifies the first signature and the change return value indicated by the message, generates a blinded second signature by signing the blinded change return certificate, and forwards the blinded second signature to the payer. The

10   payer unblinds and verifies the blinded second signature, and forms a second payment certificate. A method of performing tasks of a payer, a method of performing tasks of a payment provider in a change return transaction, and computer programs and devices therefor are also disclosed.